ELECTRICAL
& COMPUTER
ENGINEERING

ECE-595 Network Softwarization

PROF. FABRIZIO GRANELLI (FABRIZIO.GRANELLI@UNITN.IT)

PROF. MICHAEL DEVETSIKIOTIS (MDEVETS@UNM.EDU)

IEEE 802.11 Wireless LAN

802.11b

2.4 GHz unlicensed spectrum

up to 11 Mbps

direct sequence spread spectrum (DSSS) in physical layer

- all hosts use same chipping code

- all use CSMA/CA for multiple access
- all have base-station and ad-hoc network versions

802.11a

- 5–6 GHz range
- up to 54 Mbps

802.11g

- 2.4 GHz range
- up to 54 Mbps

802.11n: multiple antennae

- 2.4–5 GHz range
- up to 200 Mbps

IEEE 802.11-1997

The ORIGINAL wireless protocol.

- Security implemented via WEP
  - Wired Equivalent Privacy (Legacy)

Provided Bandwidth

- 1 or 2 Mbit/s due to use of CSMA/CA

Relatively Unpopular

Low interoperability due to loose specifications

Used DSSS

Considered Legacy and no longer used

IEEE 802.11a

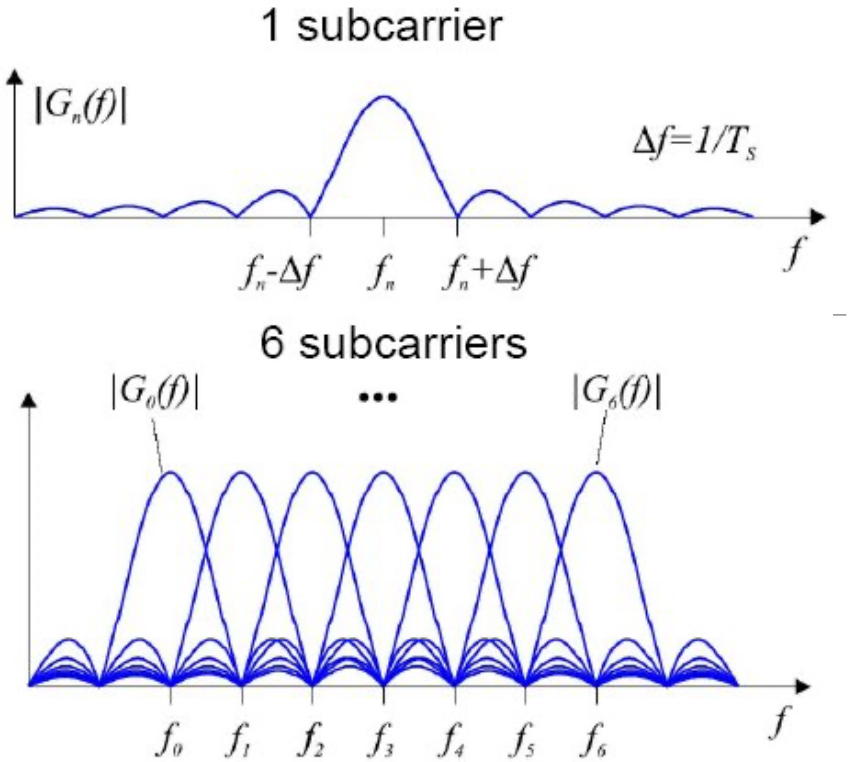
One of two amendments to the original 802.11 specification released simultaneously

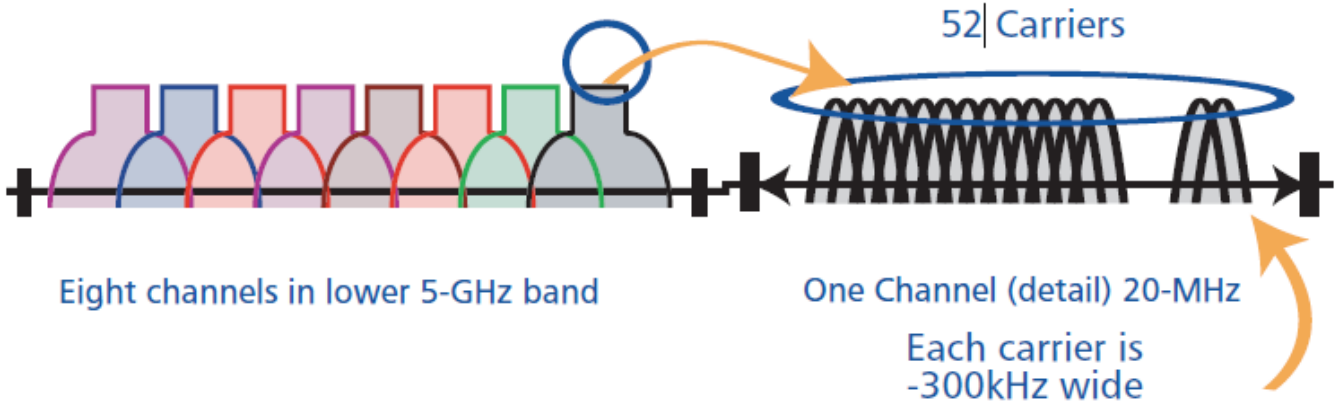
Provided up to 54 Mbit/s bandwidth

Uses OFDM

- Orthogonal Frequency-Division Multiplexing
  - Transmits a signal over several sub signals for higher efficiency

OFDM


1 subcarrier
$|G_n(f)|$
$\Delta f=1/T_S$
f_n-Δf
f_n
f_n+Δf
f
6 subcarriers
$|G_0(f)|$
$|G_6(f)|$
f_0 f_1 f_2 f_3 f_4 f_5 f_6
f


52 Carriers
Eight channels in lower 5-GHz band
One Channel (detail) 20-MHz
Each carrier is
-300kHz wide

IEEE 802.11b

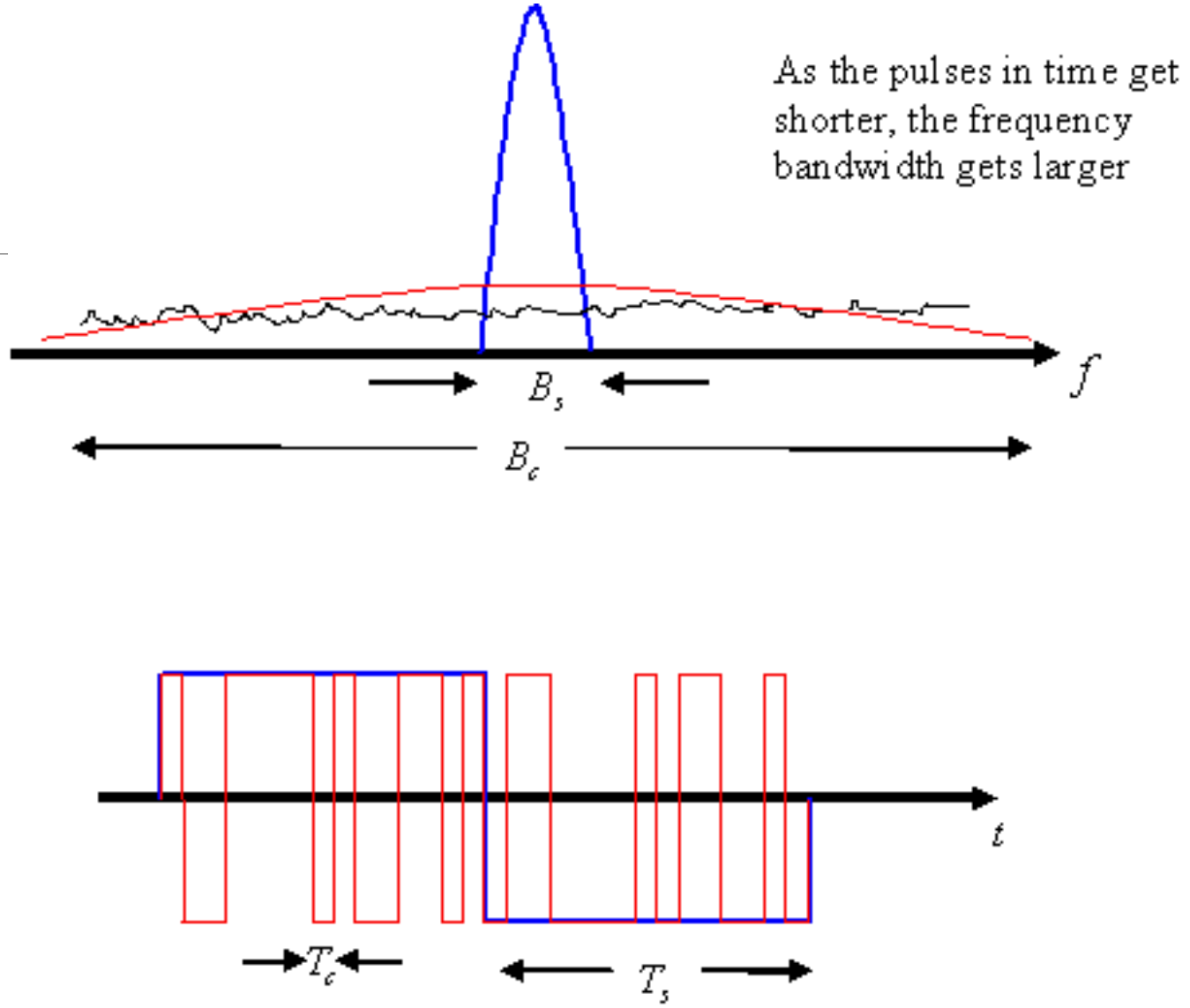
Second of two amendments released in 1999

Provided up to 11 Mbit/s bandwidth

Uses DSSS

- Direct-Sequence Spread Spectrum
  - Transmits a signal over several sub signals for higher efficiency

DSSS


As the pulses in time get shorter, the frequency bandwidth gets larger
B_s
B_c
f
t
T_c
T_s

IEEE 802.11a and b

Both introduced at the same time

Both use CSMA/CA

802.11a

- Faster
- More expensive to manufacture
- Operated in 5Ghz band
- Mainly used in industrial settings

802.11b

- Slower
- Cheaper to manufacture
- Operated in 2.4Ghz band.
- Mainly used in residential settings

IEEE 802.11g

The most common wireless network in use before .11n.

Operates on 2.4Ghz band

Provides up 54Mbit/s bandwidth

- 108Mbit/s with special implementations

Uses OFDM for modulation

Adopted quickly after release for cheap and high bandwidth

IEEE 802.11n

Reference version of the 802.11 family.

Has rated 600Mbit/s bandwidth

Introduces MIMO

- Multiple-Input Multiple-Output

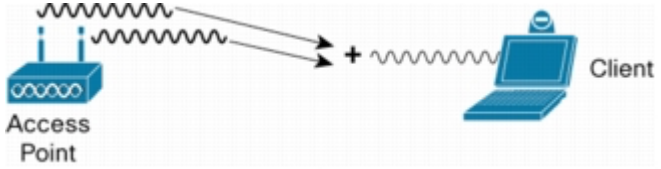
OFDM Modulation

- Uses higher frequencies for increased number of carrier waves

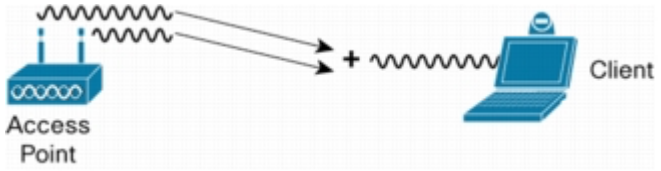
IEEE 802.11n – New Technologies

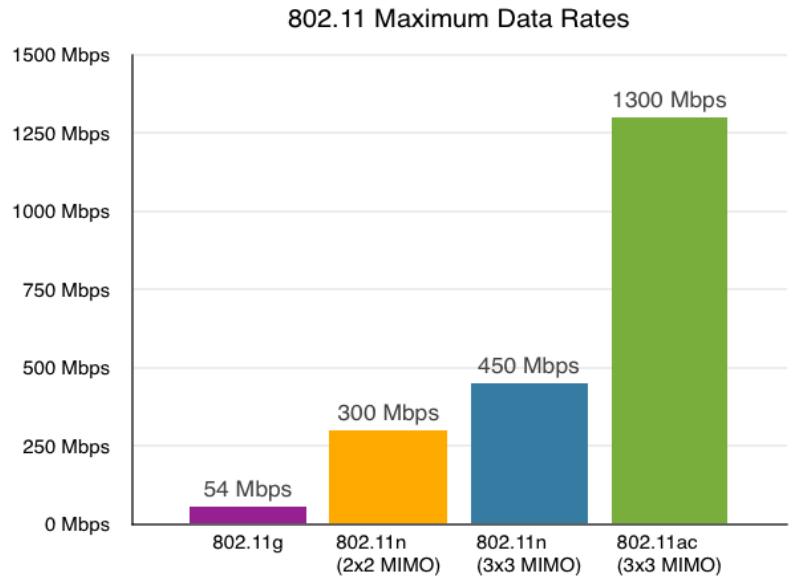
Beam Forming

- Takes advantage of multi-antenna setup
- Makes signals from separate antenna arrive in sync
- Out of sync leads to interference



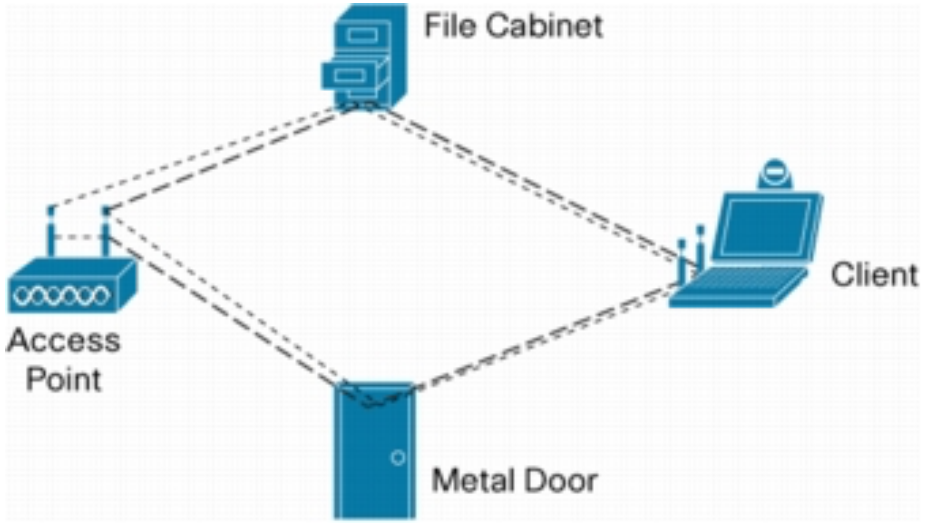
- In sync leads to greater signal strength





IEEE 802.11n – New Technologies

Multipath/Spatial Diversity



- Multiple antenna/radios send/receive signals
- Different signals reach receivers at different times
- Use math to combine signals for greater quality
- Each stream can carry separate data

IEEE 802.11n – New Technologies

Guard interval reduction

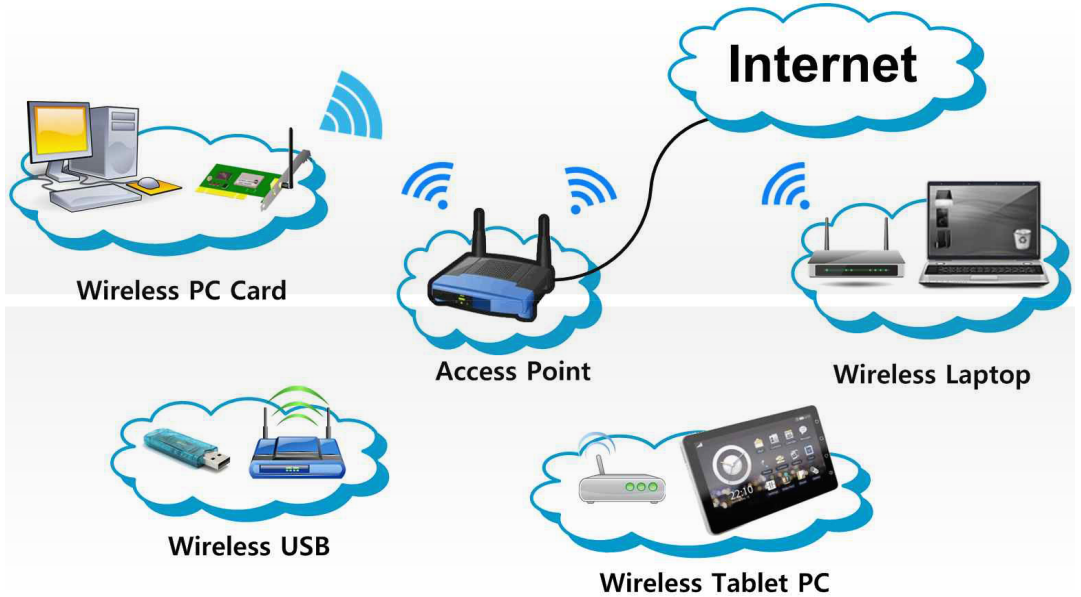
- Guard interval is a time of radio silence
- Used to avoid interference
- 802.11n can reduce guard interval from 800μs to 400μs.

Frame aggregation

- Aggregate multiple frames destined for a specific AP and send them together to reduce overhead

IEEE 802.11 LAN architecture

Infrastructure mode



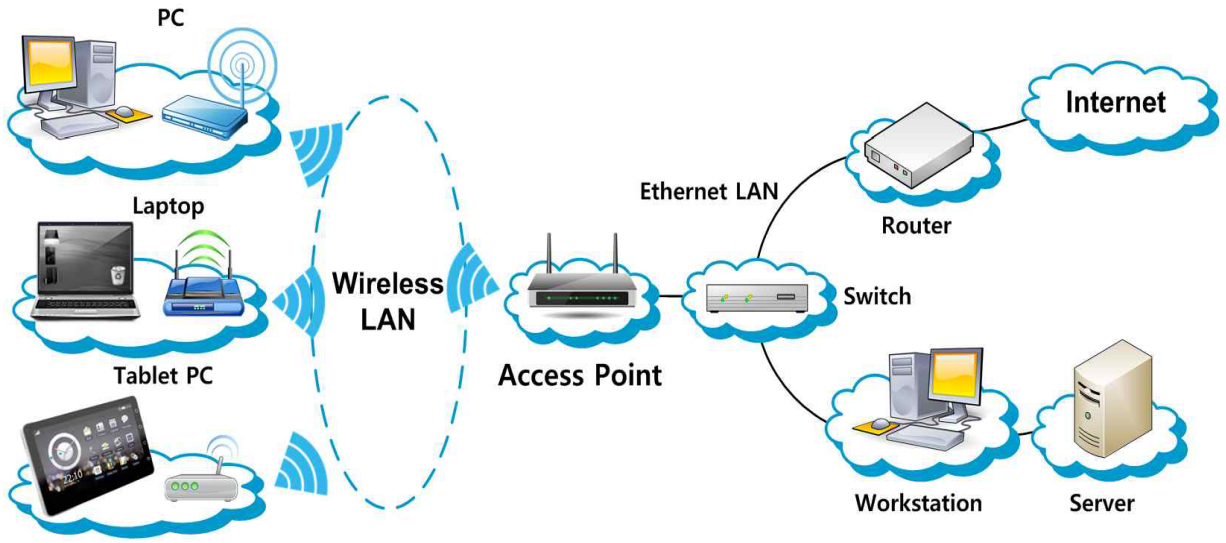
Infrastructure Mode

- In infrastructure mode, Wi-Fi devices can
  - communicate with each other and
  - communicate with a wired network

- BSS (Basic Service Set)
  - In infrastructure mode, commonly one AP is connected by wire to the Internet, and a set of Wi-Fi devices connect to the AP

IEEE 802.11 LAN architecture

Another example of Infrastructure mode

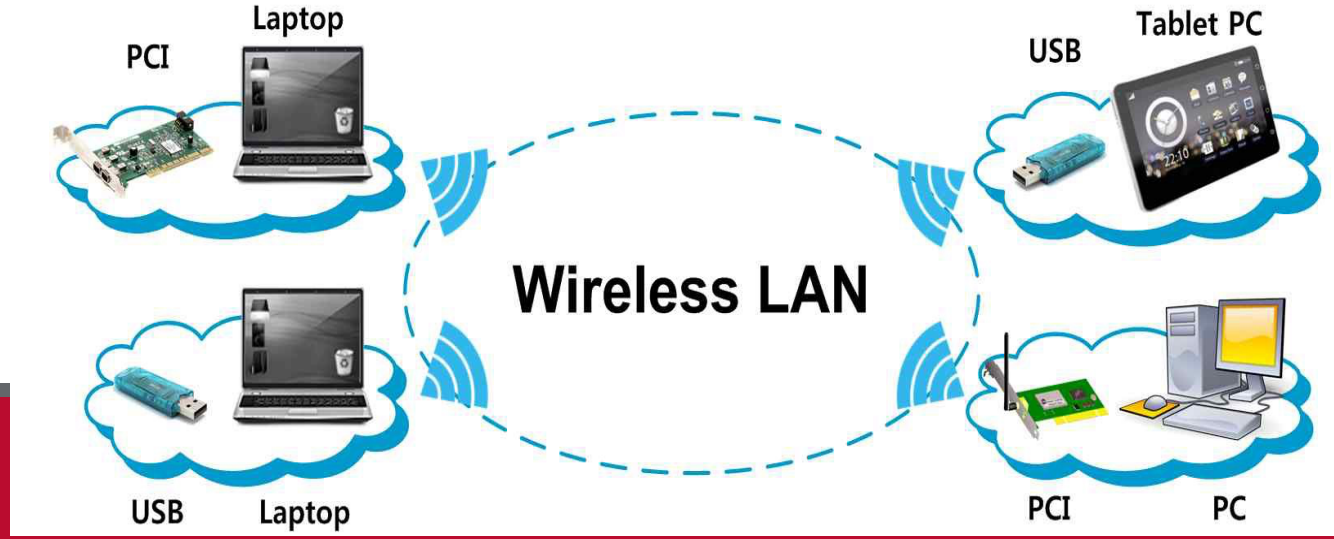


IEEE 802.11 LAN architecture

Ad-Hoc Mode

- Wi-Fi devices or stations communicate directly with each other, without help from an AP (Access Point) ➔ Used where Infrastructure Mode network setup is not needed or not possible
- Also referred to as peer-to-peer mode
- IBSS (Independent Basic Service Set)
  - Ad-hoc mode network is referred to as an IBSS

Example of Ad-Hoc mode

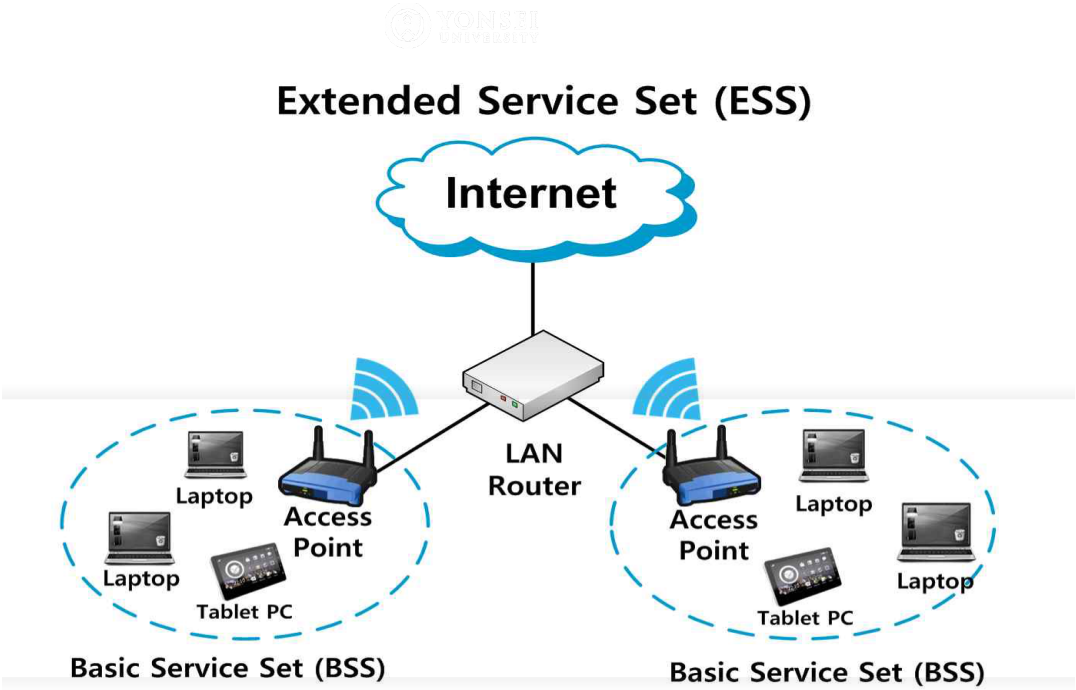


IEEE 802.11 LAN architecture

BSS & ESS

- BSS (Basic Service Set) is the basic building block of an 802.11 WLAN
  - In infrastructure mode, a BSS is formed by a single AP (Access Point) and all associated STAs (stations)
  - AP acts as a Master and controls all STAs within the BSS
- ESS (Extended Service Set) is a set of two or more BSSs that form a single network

➔ Extends the range of Wi-Fi STA mobility



IEEE 802.11 Versions

IEEE 802.11 Network PHY Standards (1/2)				
802.11 Protocol	Release Date	Frequency	Bandwidth	Stream Data Rate
802.11-1997	Jun. 1997	2.4 GHz	22 MHz	1, 2 Mbps
802.11a	Sep. 1999	5 GHz	20 MHz	6 ~ 54 Mbps
		3.7 GHz		
802.11b	Sep. 1999	2.4 GHz	22 MHz	1 ~ 11 Mbps
802.11g	Jun. 2003	2.4 GHz	20 MHz	6 ~ 54 Mbps
802.11n	Oct. 2009	2.4/5 GHz	20 MHz	7.2 ~ 72.2 Mbps
			40 MHz	15 ~ 150 Mbps

IEEE 802.11 Versions

IEEE 802.11 Network PHY Standards (2/2)				
802.11 Protocol	Release Date	Frequency	Bandwidth	Stream Data Rate
802.11ac	Dec. 2013	5 GHz	20 MHz	7.2 ~ 96.3 Mbps
			40 MHz	15 ~ 200 Mbps
			80 MHz	32.5 ~ 433.3 Mbps
			160 MHz	65 ~ 866.7 Mbps
802.11ad	2012, 2016	60 GHz	2.16 GHz	Up to 7 Gbps
802.11ay	2017	60 GHz	8 GHz	Up to 100 Gbps

IEEE 802.11 Versions

IEEE 802.11 Network PHY Standards (1/2)				
802.11 protocol	Frequency	Modulation	Approximate Range	
			Indoor (m)	Outdoor (m)
802.11-1997	2.4 GHz	DSSS, FHSS	20	100
802.11a	5 GHz	OFDM	35	120
	3.7 GHz		–	5000
802.11b	2.4 GHz	DSSS	35	140
802.11g	2.4 GHz	OFDM, DSSS	38	140

IEEE 802.11 Versions

IEEE 802.11 Network PHY Standards (2/2)				
802.11 protocol	Frequency	Modulation	Approximate Range	
			Indoor (m)	Outdoor (m)
802.11n	2.4/5 GHz	OFDM (MIMO-4)*	70	250
802.11ac	5 GHz	OFDM (MIMO-8)*	35	-
802.11ad	60 GHz	OFDM (>10X10 MIMO)	10	10

*MIMO-4 and MIMO-8 represent that the allowable MIMO streams are 4 and 8, respectively.

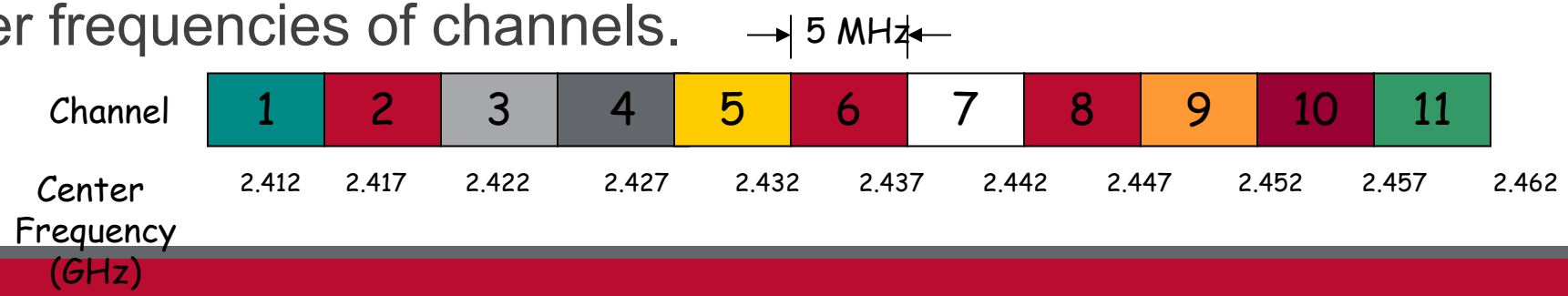
IEEE 802.11b Channels

802.11 splits up the frequencies within the band into 14 radio channels, numbered 1-14.

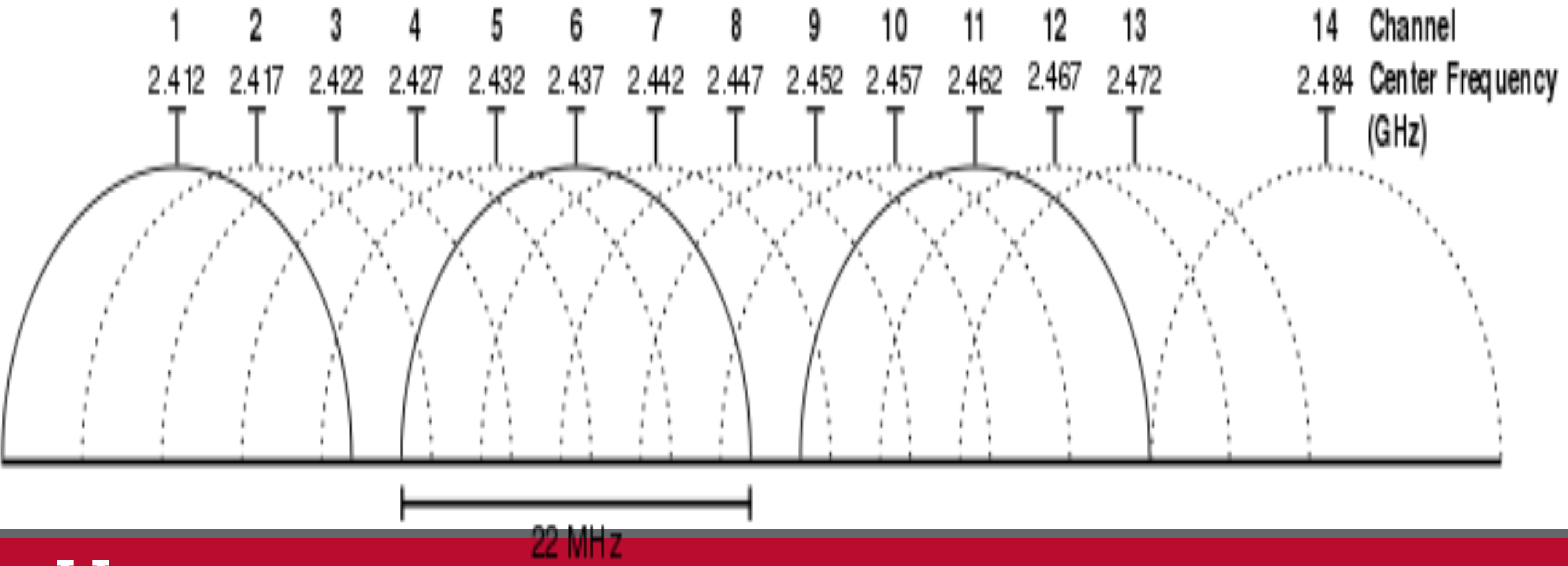
These are the 14 channels designated in the 2.4 GHz range spaced 5 MHz apart (with the exception of a 12 MHz spacing before Channel 14).

FCC allows channels 1 through 11 within the U.S. Most of Europe can use channels 1 through 13. In Japan, only 1 choice: channel 14.

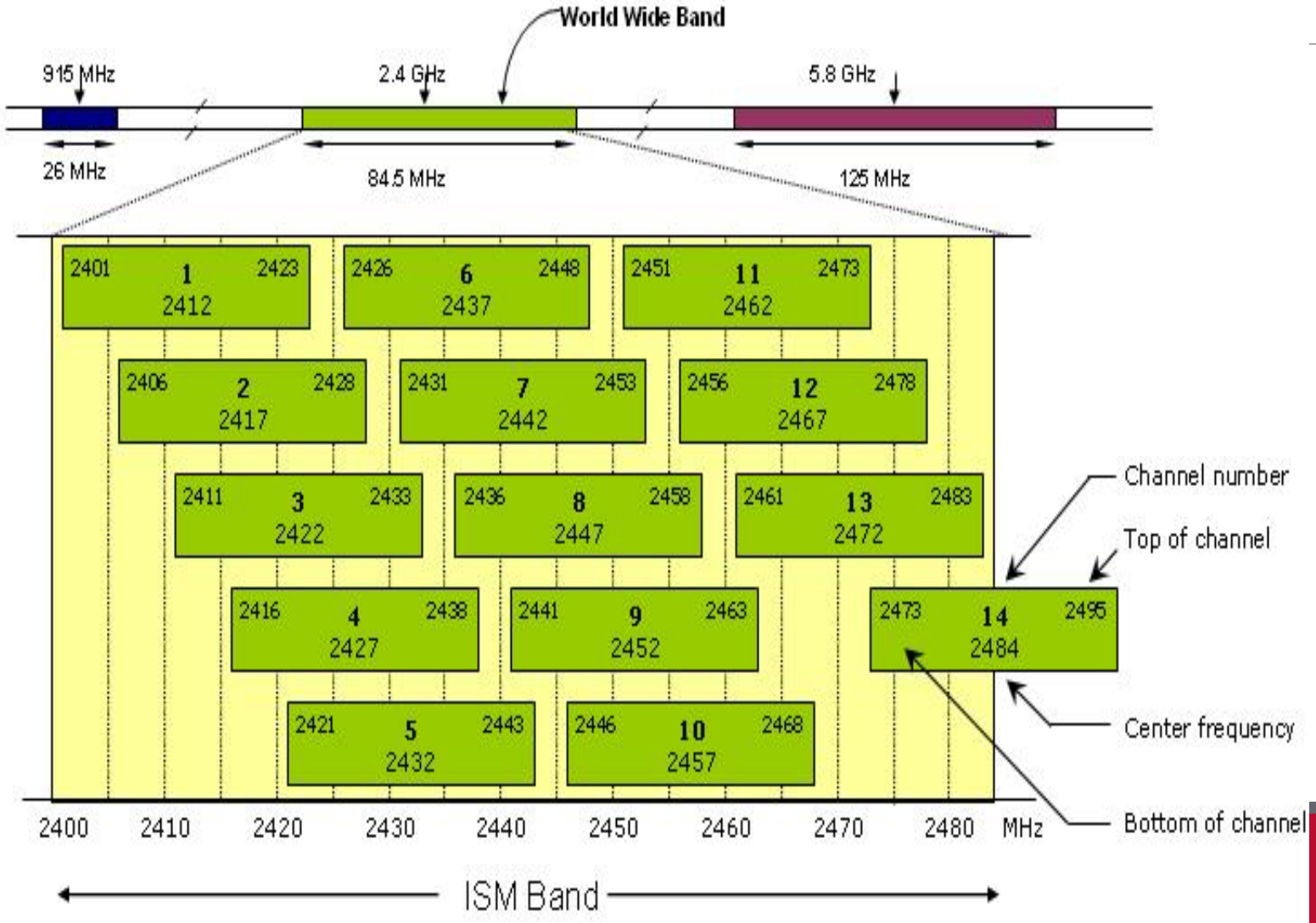
Channel represents a center frequency. Only 5 MHz separation between center frequencies of channels.



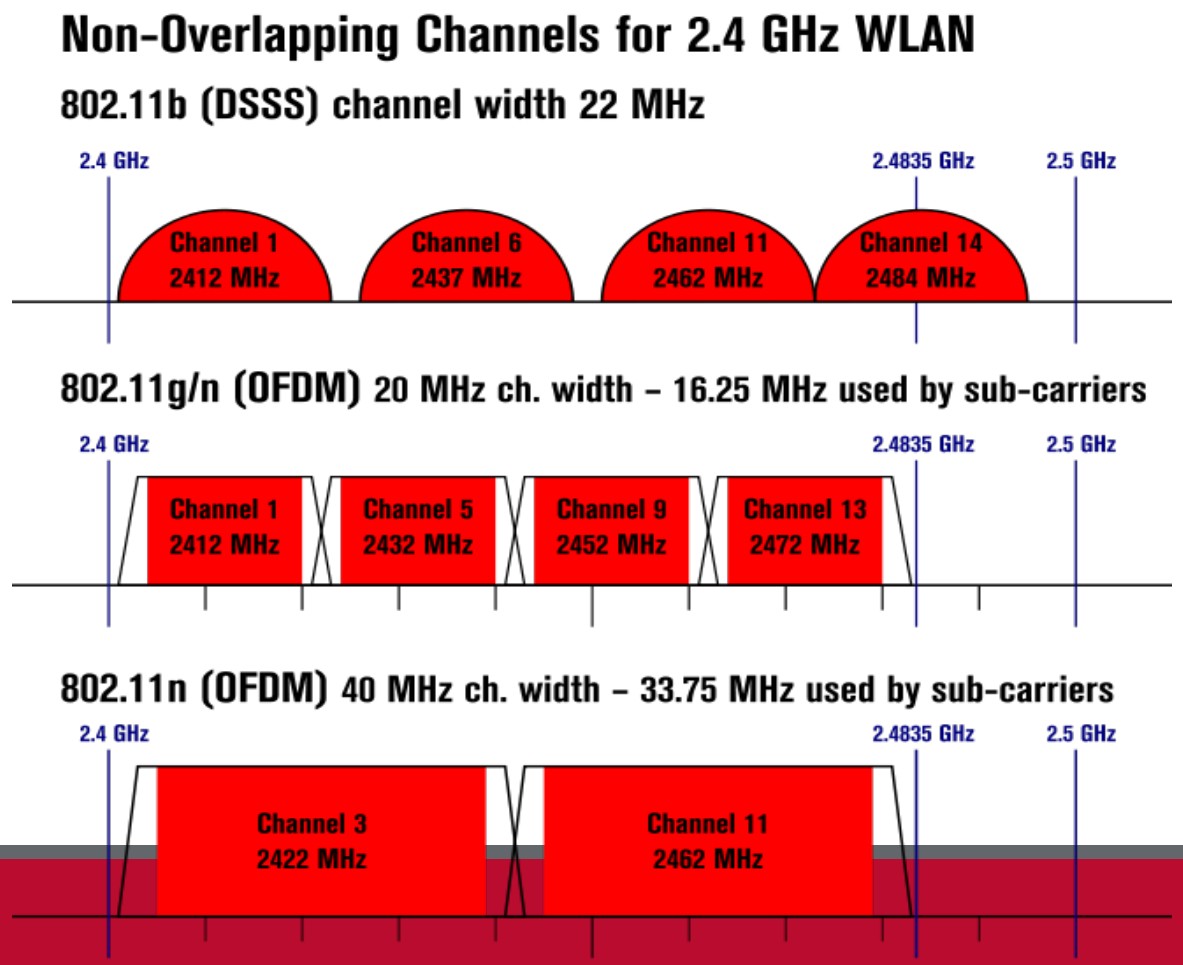
IEEE 802.11b Channels



IEEE 802.11b Channels

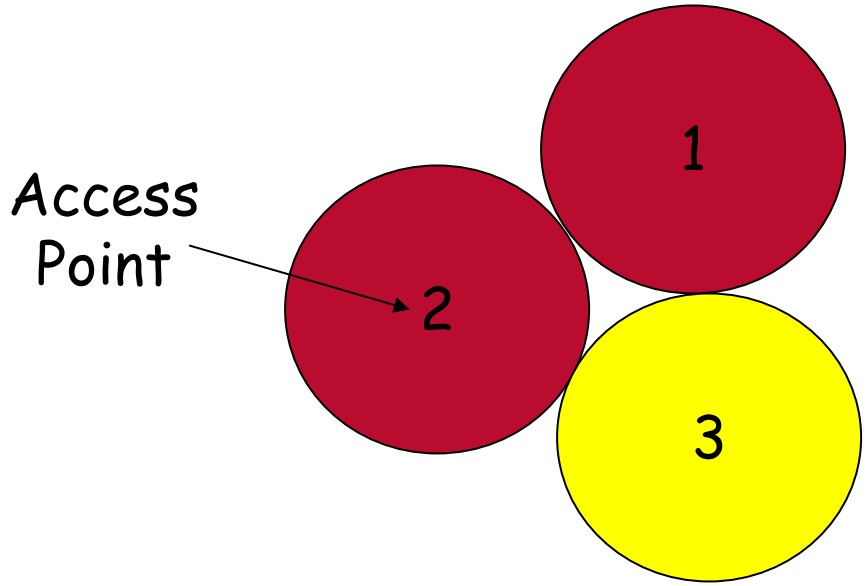


2.4 GHz (IEEE 802.11b/g/n)



IEEE 802.11b (Cont'd)

Neighboring AP's use different channels to reduce interference. "Reuse cluster" size is equal to 3.



WiFi Direct

Wi-Fi Direct

- Wi-Fi Direct devices can connect directly to one another without access to a traditional network

- Devices can make a one-to-one connection, or a group of several devices can connect simultaneously

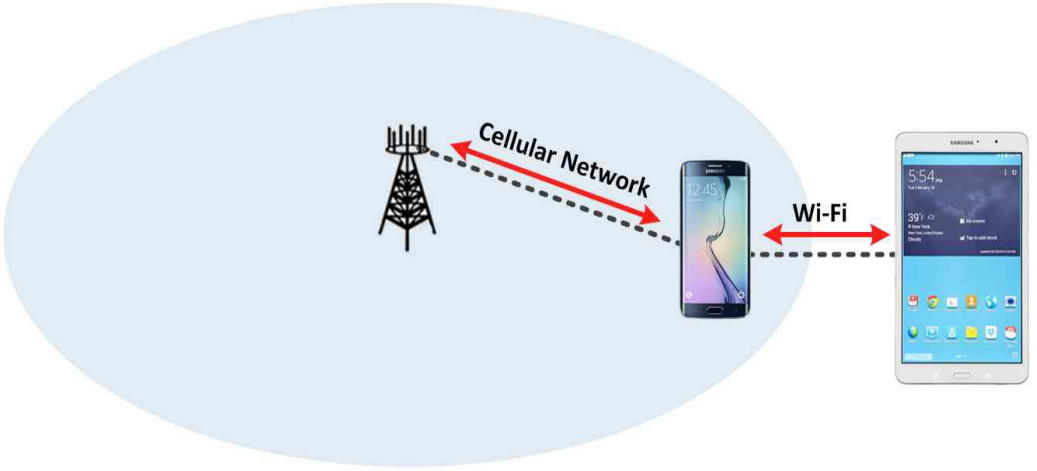
- With optional services, users can send files, print documents, play media, and display screens between and among devices

WiFi Tethering (Hotspot)

- **Tethering** refers to connecting one device to another

- In the context of mobile phones or Internet tablets, tethering allows **sharing the Internet connection** of the phone or tablet with other devices such as laptops

- A Wi-Fi STA can make connection to the Internet by connecting to a smartphone using Wi-Fi



IEEE 802.11: Channels, Association

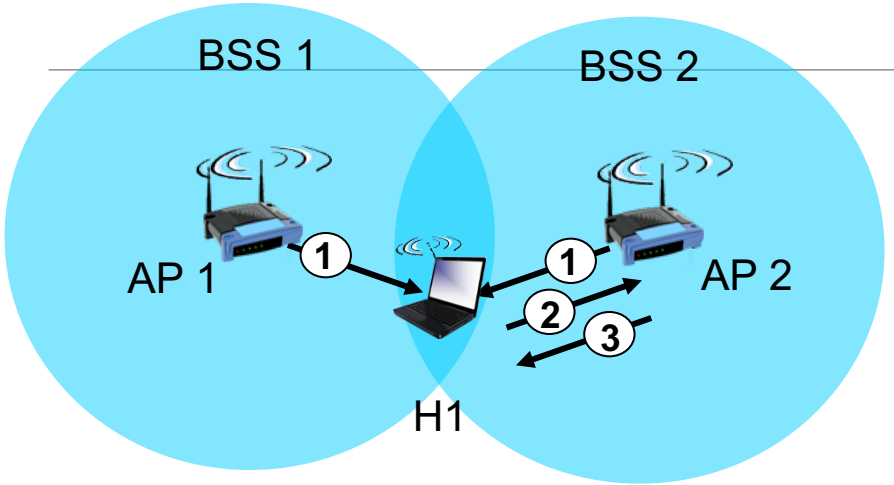
802.11b: 2.4GHz-2.485GHz spectrum divided into 11 channels at different frequencies

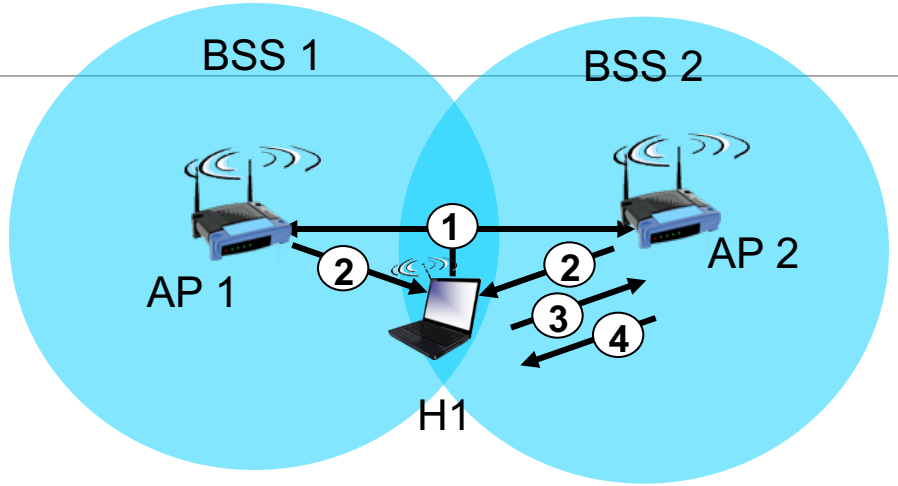
- AP admin chooses frequency for AP
- interference possible: channel can be same as that chosen by neighboring AP!

host: must *associate* with an AP

- scans channels, listening for *beacon frames* containing AP's name (SSID) and MAC address
- selects AP to associate with
- may perform authentication
- will typically run DHCP to get IP address in AP's subnet

IEEE 802.11: Scanning





passive scanning:

(1) beacon frames sent from APs
(2) association Request frame sent: H1 to selected AP
(3) association Response frame sent from selected AP to H1

active scanning:

(1) Probe Request frame broadcast from H1
(2) Probe Response frames sent from APs
(3) Association Request frame sent: H1 to selected AP
(4) Association Response frame sent from selected AP to H1

IEEE 802.11: Multiple Access

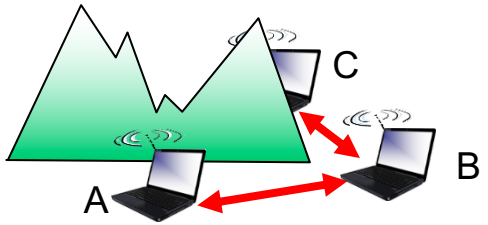
avoid collisions: 2^+ nodes transmitting at same time

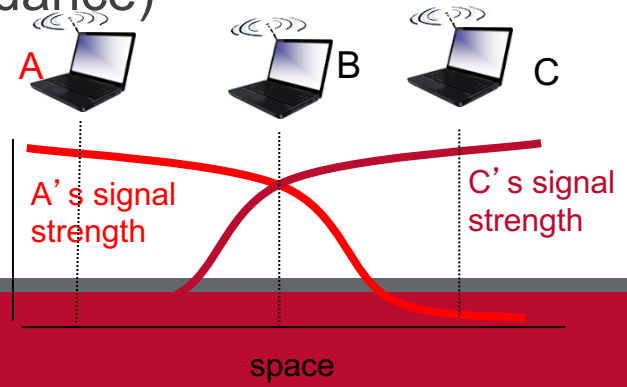
802.11: CSMA - sense before transmitting

- don't collide with ongoing transmission by other node

802.11: *no* collision detection!

- difficult to receive (sense collisions) when transmitting due to weak received signals (fading)
- can't sense all collisions in any case: hidden terminal, fading
- goal: *avoid collisions:* CSMA/C(ollision)A(voidance)





IEEE 802.11 MAC: CSMA/CA

802.11 sender

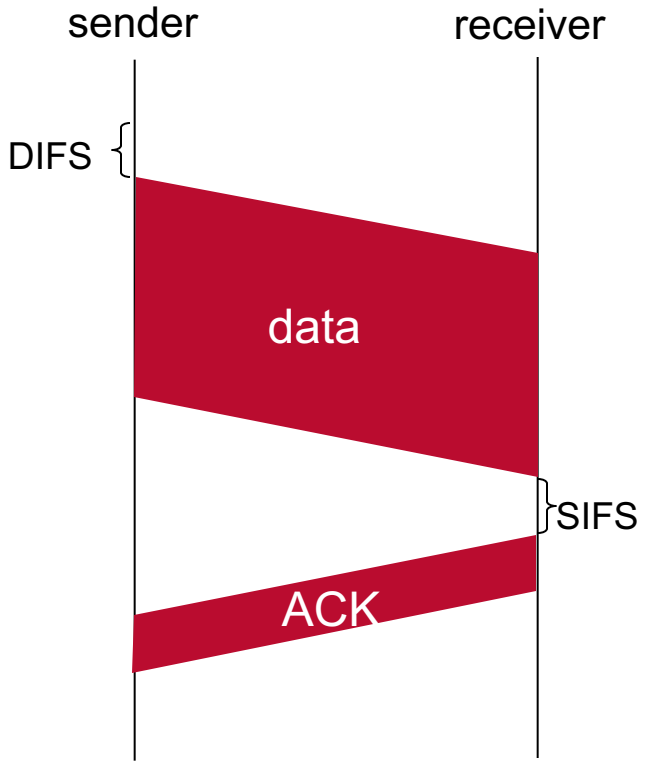
1 if sense channel idle for **DIFS - Distributed Inter Frame Space** then
transmit entire frame (no CD)

2 if sense channel busy then
start random backoff time
timer counts down while channel idle
transmit when timer expires
if no ACK, increase random backoff interval, repeat 2

802.11 receiver

- if frame received OK

return ACK after **SIFS – Short Inter Frame Space** (ACK needed due to hidden terminal problem)



Avoiding collisions (more)

idea: allow sender to "reserve" channel rather than random access of data frames: avoid collisions of long data frames

sender first transmits *small* request-to-send (RTS) packets to BS using CSMA

- RTSs may still collide with each other (but they're short)

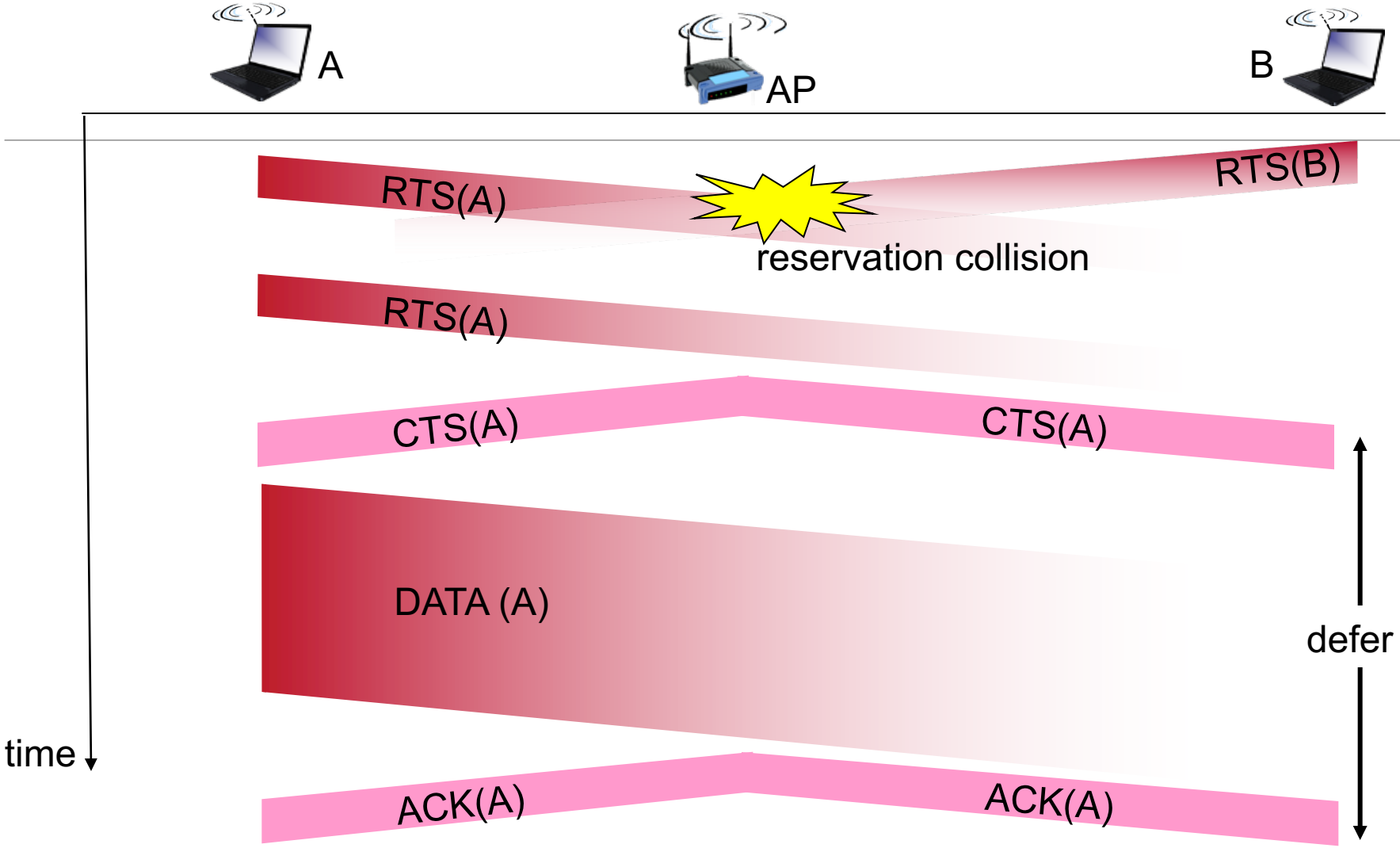
BS broadcasts clear-to-send CTS in response to RTS

CTS heard by all nodes

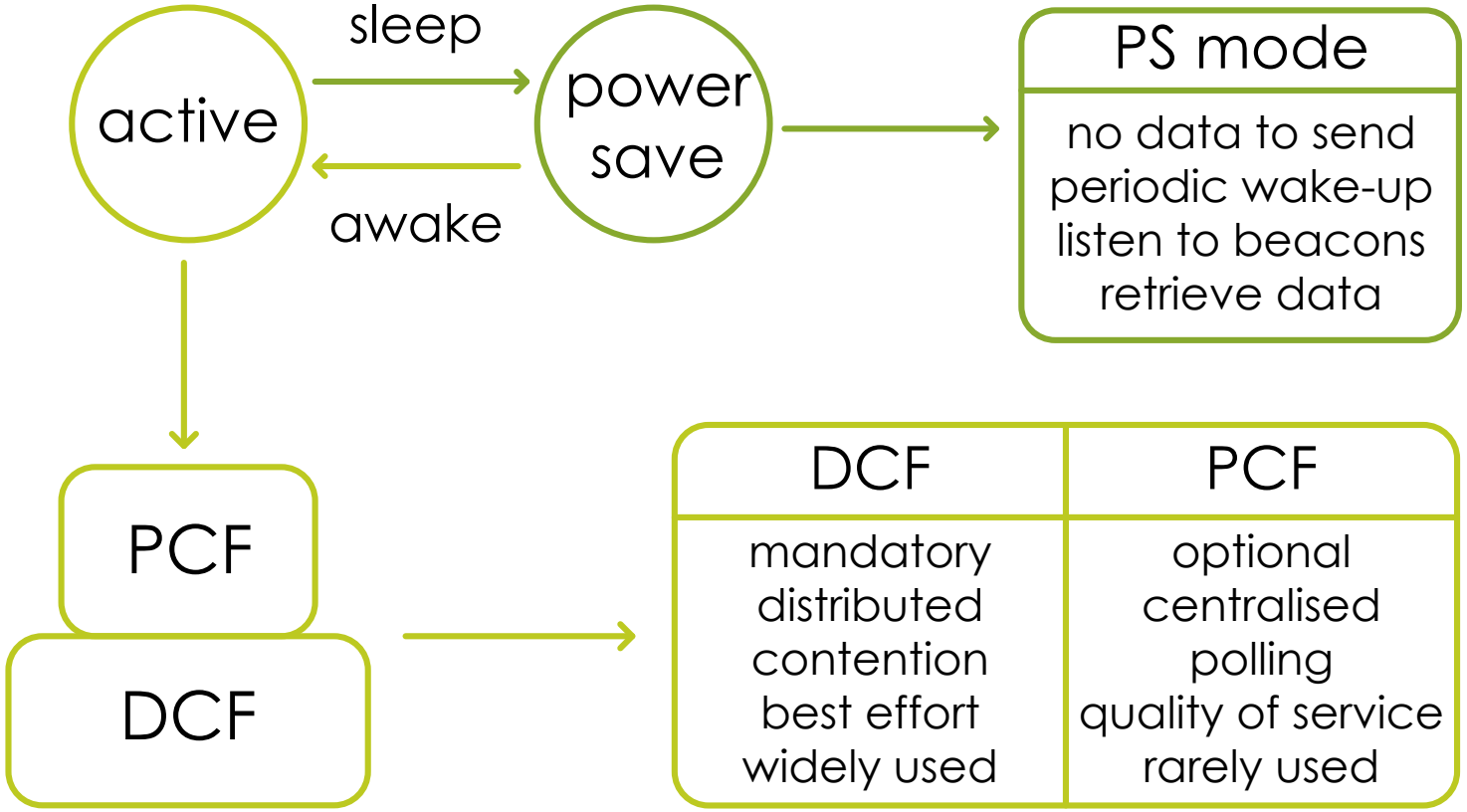
- sender transmits data frame
- other stations defer transmissions

avoid data frame collisions completely
using small reservation packets!

Collision Avoidance: RTS/CTS

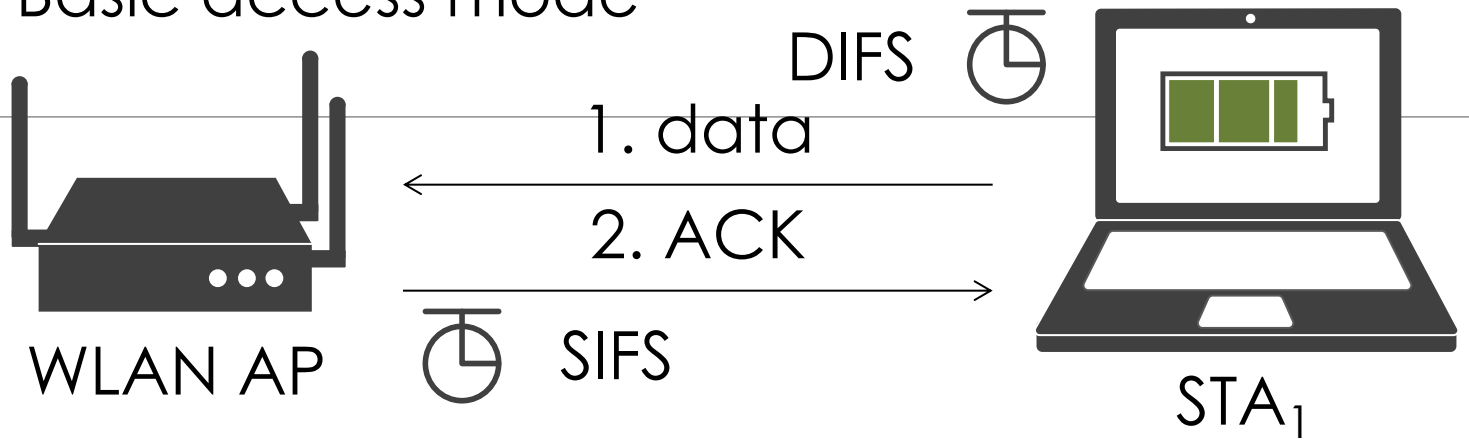


IEEE 802.11a/b/g MAC layer

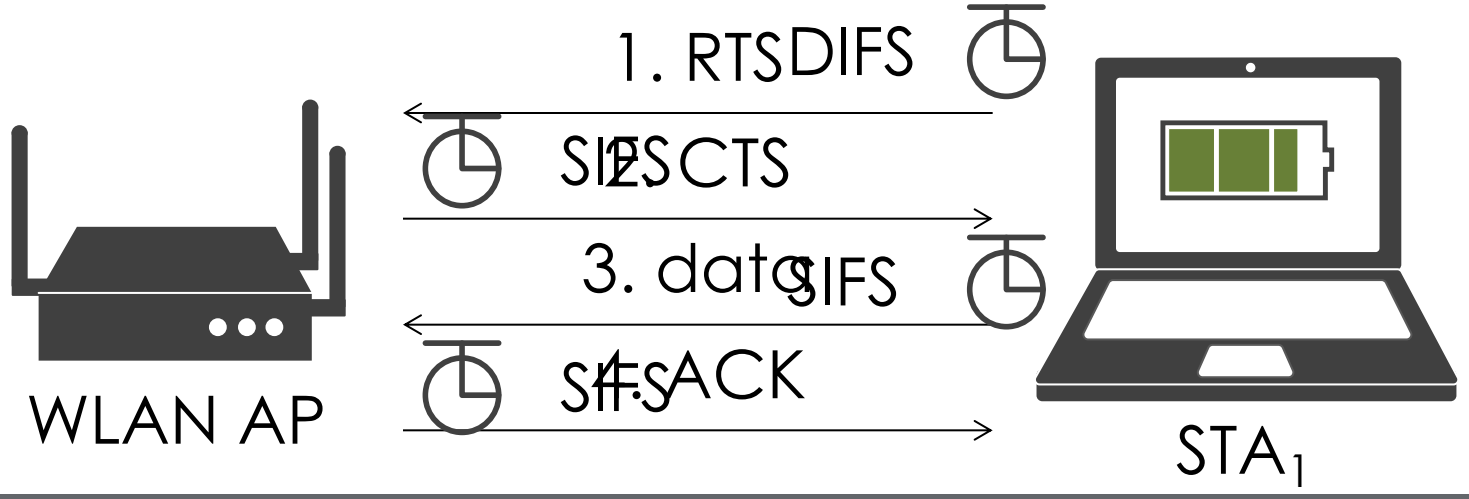


DCF: Access Modes

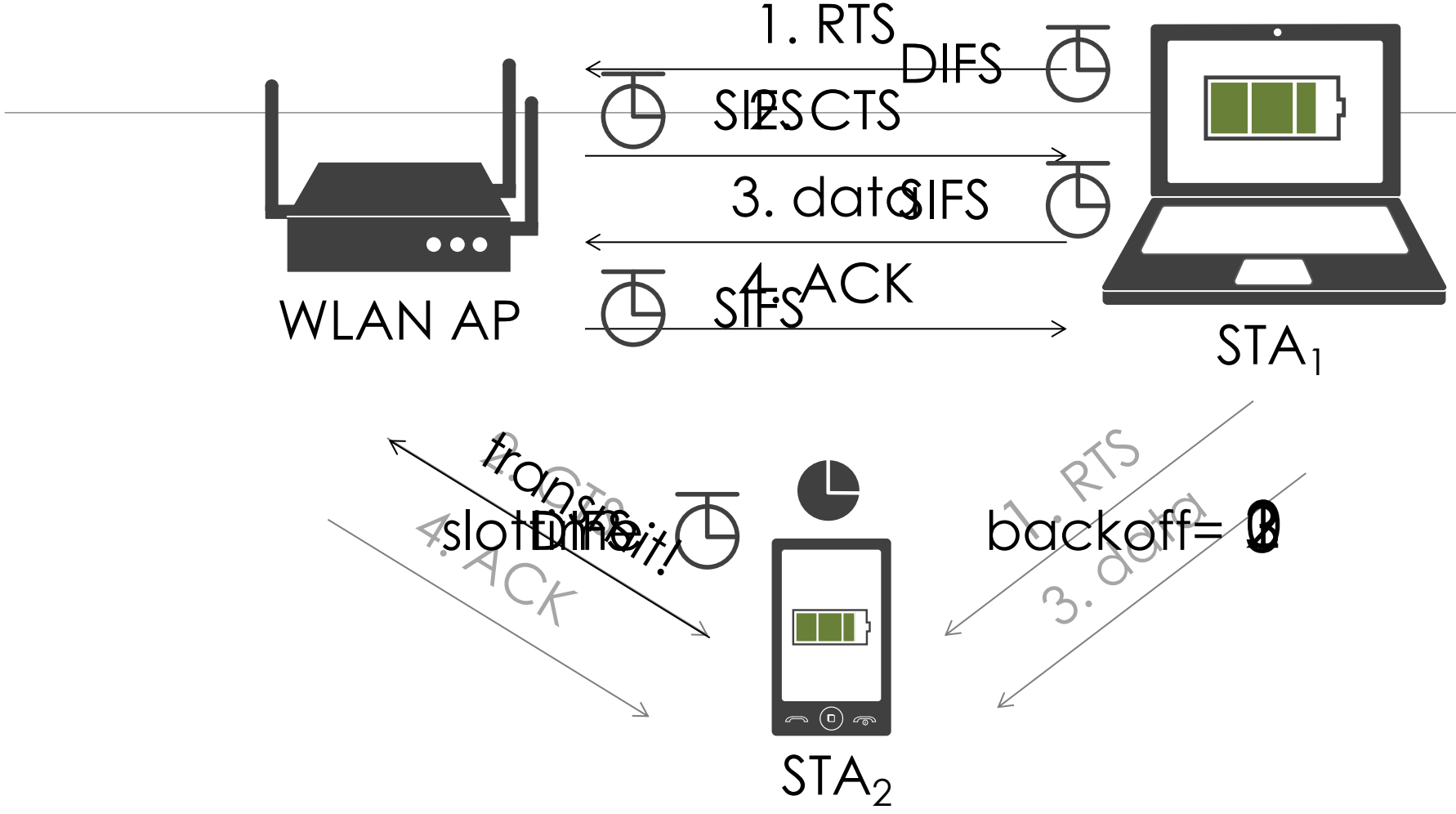
Basic access mode



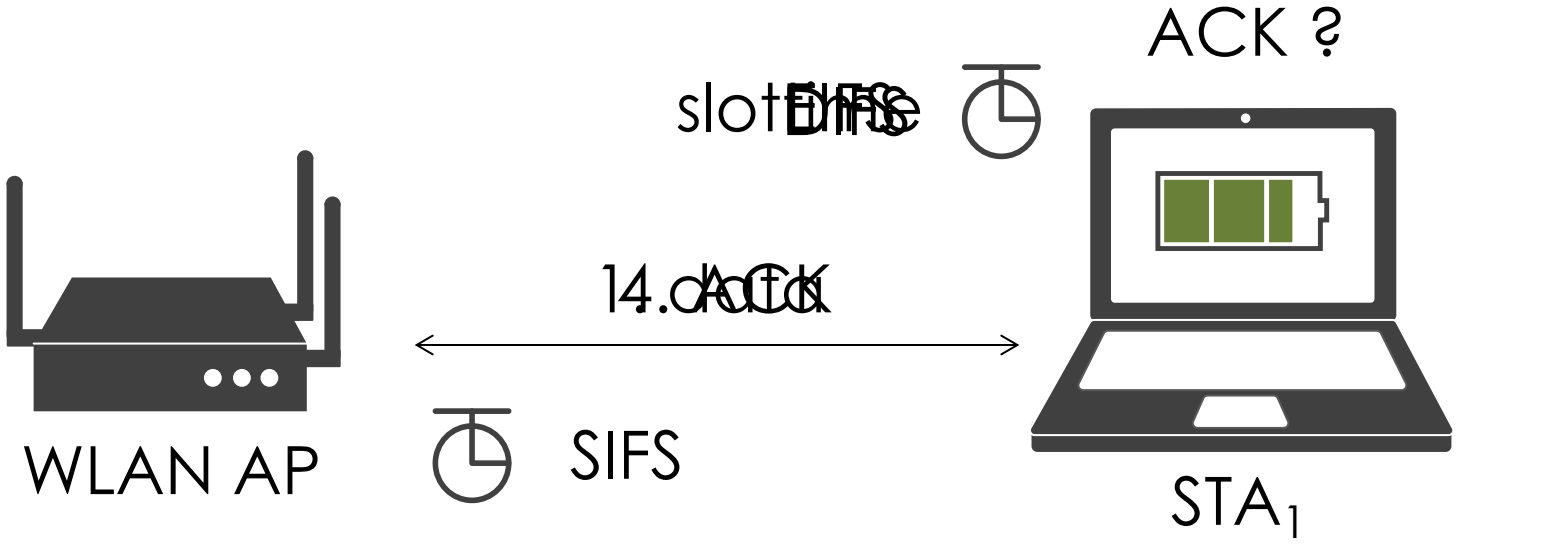
Collision avoidance access mode



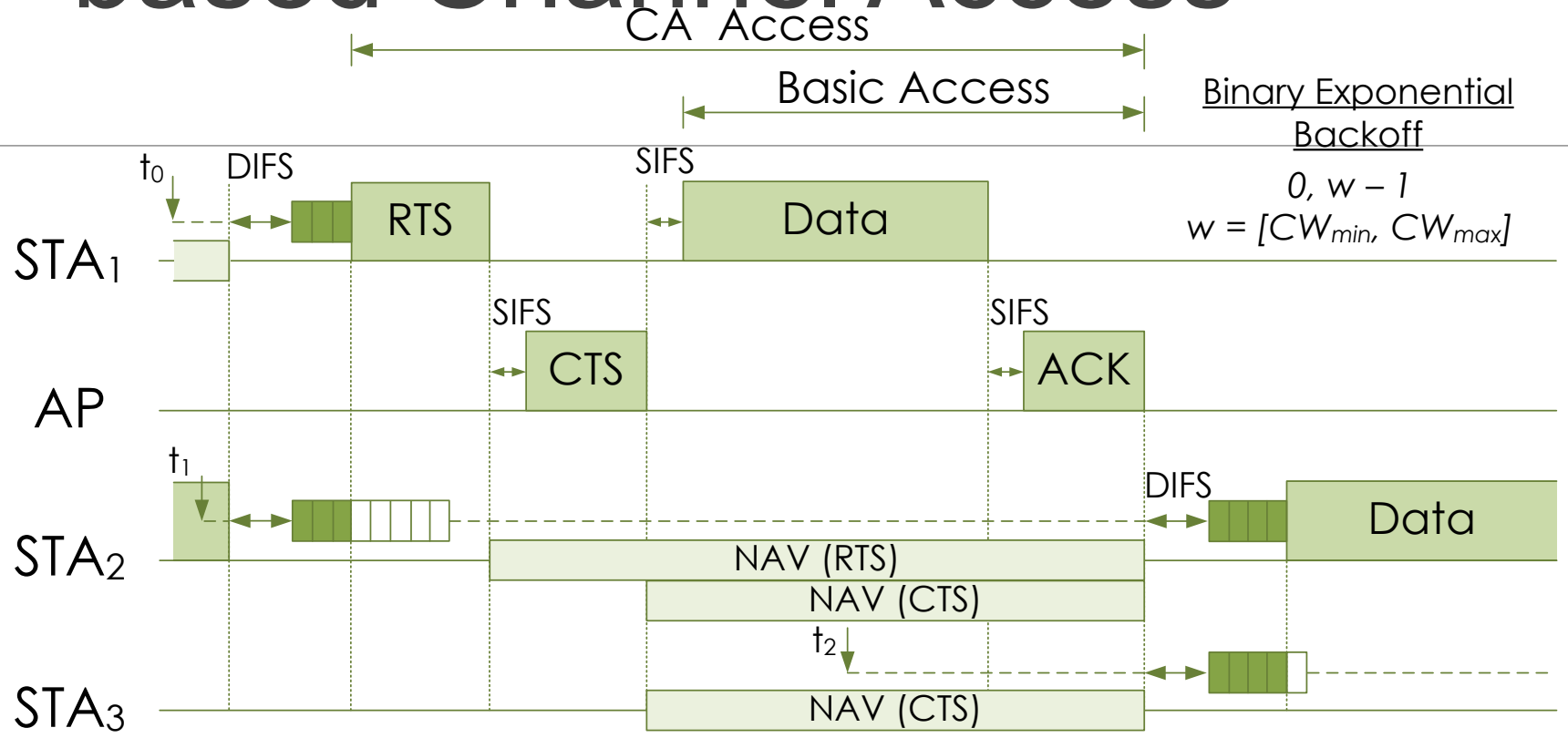
DCF: Virtual Sensing



DCF: Binary Exponential Backoff

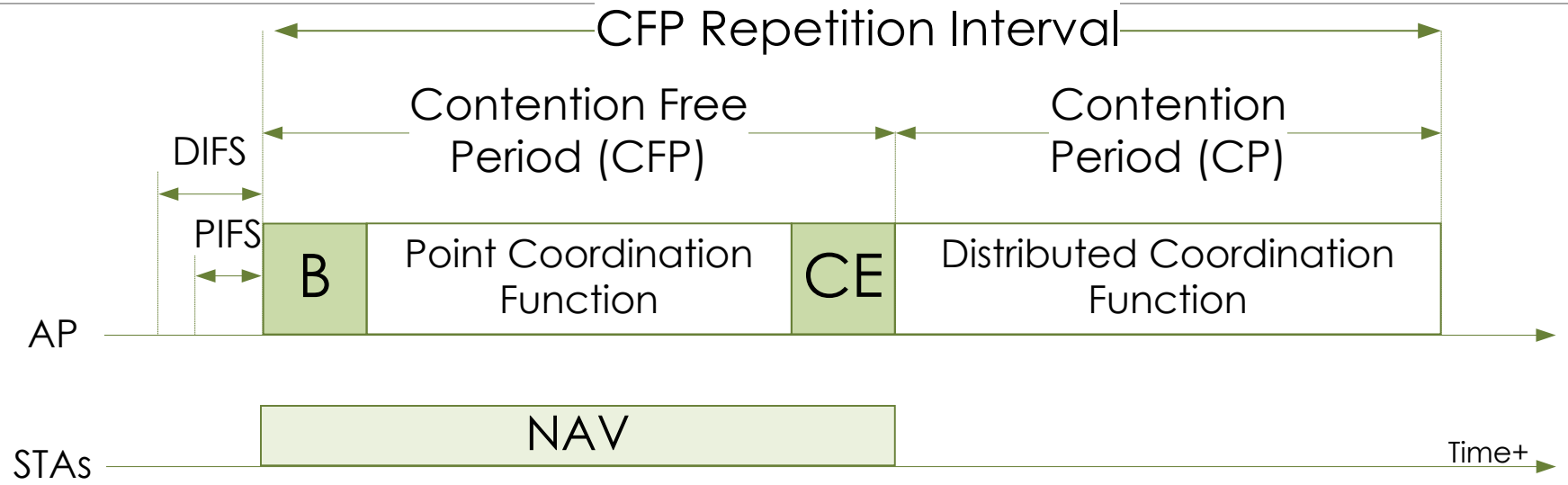


DCF-based Channel Access



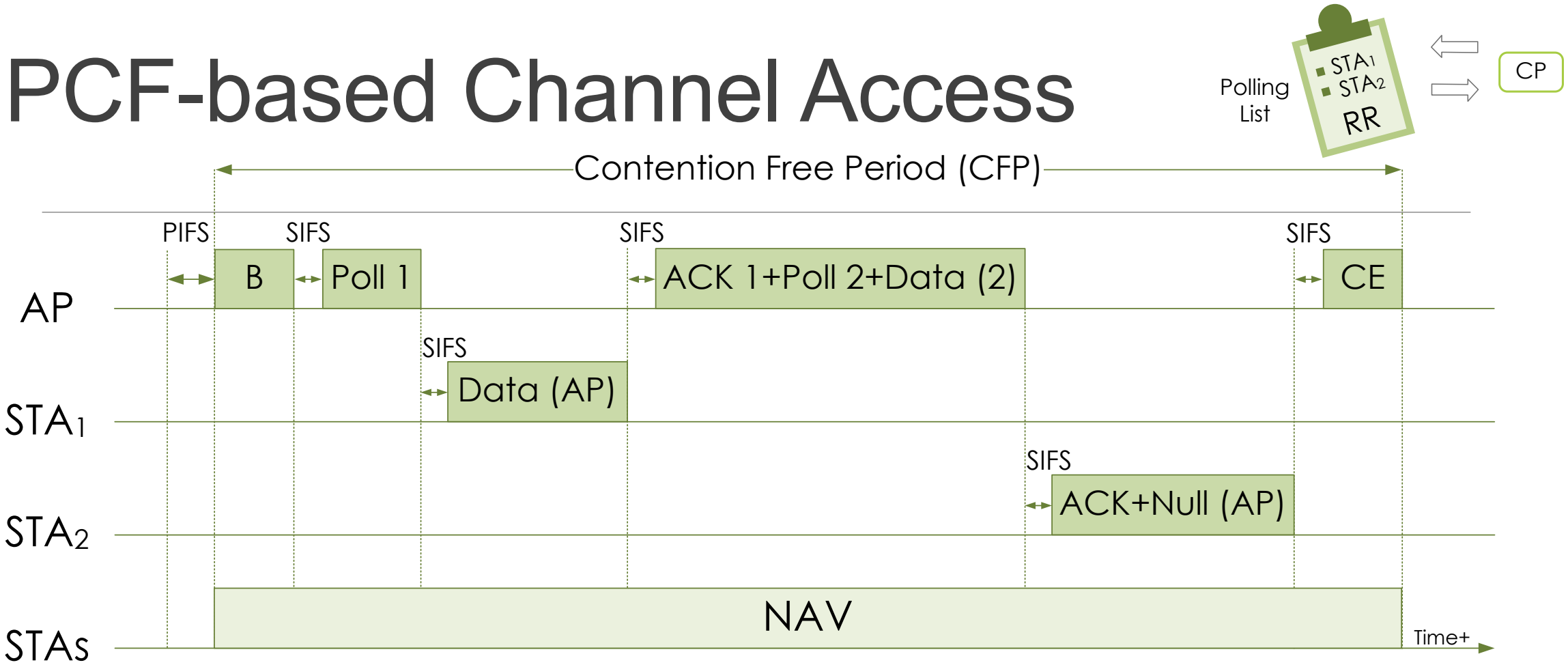
The stations must sense channel activity before transmitting. When the wireless channel is sensed busy, a backoff process of random duration is executed to avoid packet collisions.

Coexistence of PCF and DCF



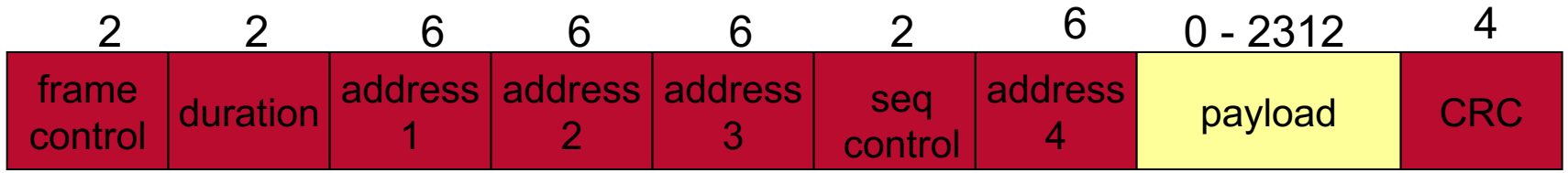
When the PCF is executed, the AP announces a periodic super structure in which the channel access time is divided into CFPs, wherein the PCF is used, and CPs, wherein the DCF is employed.

PCF-based Channel Access



The AP delivers data and sequentially polls the mobile stations of the polling list to grant them transmission opportunities. The mobile stations join and leave the polling list via the DCF in CPs.

IEEE 802.11 Frame Format



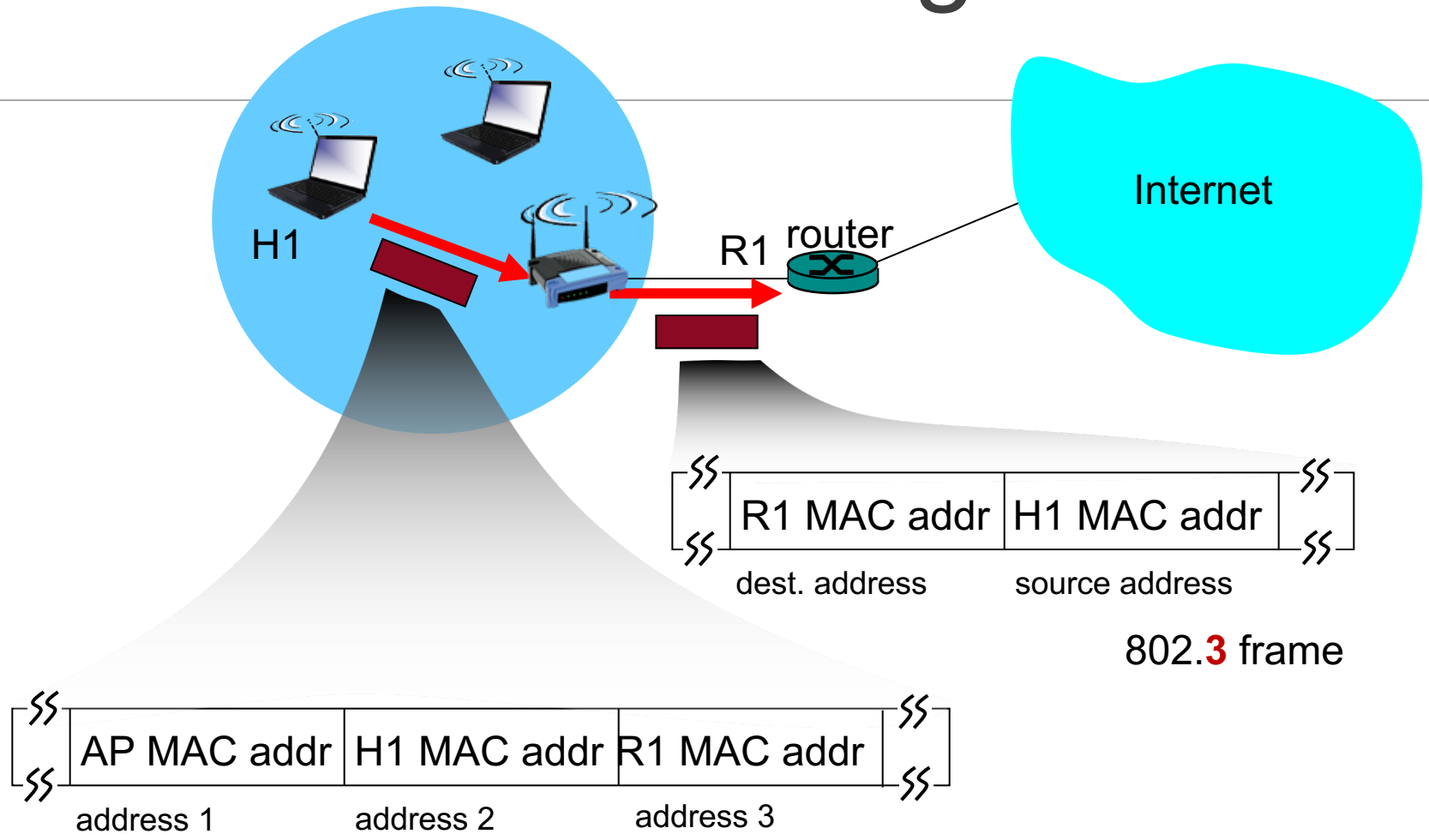
Address 1: MAC address of wireless host or AP to receive this frame

Address 2: MAC address of wireless host or AP transmitting this frame

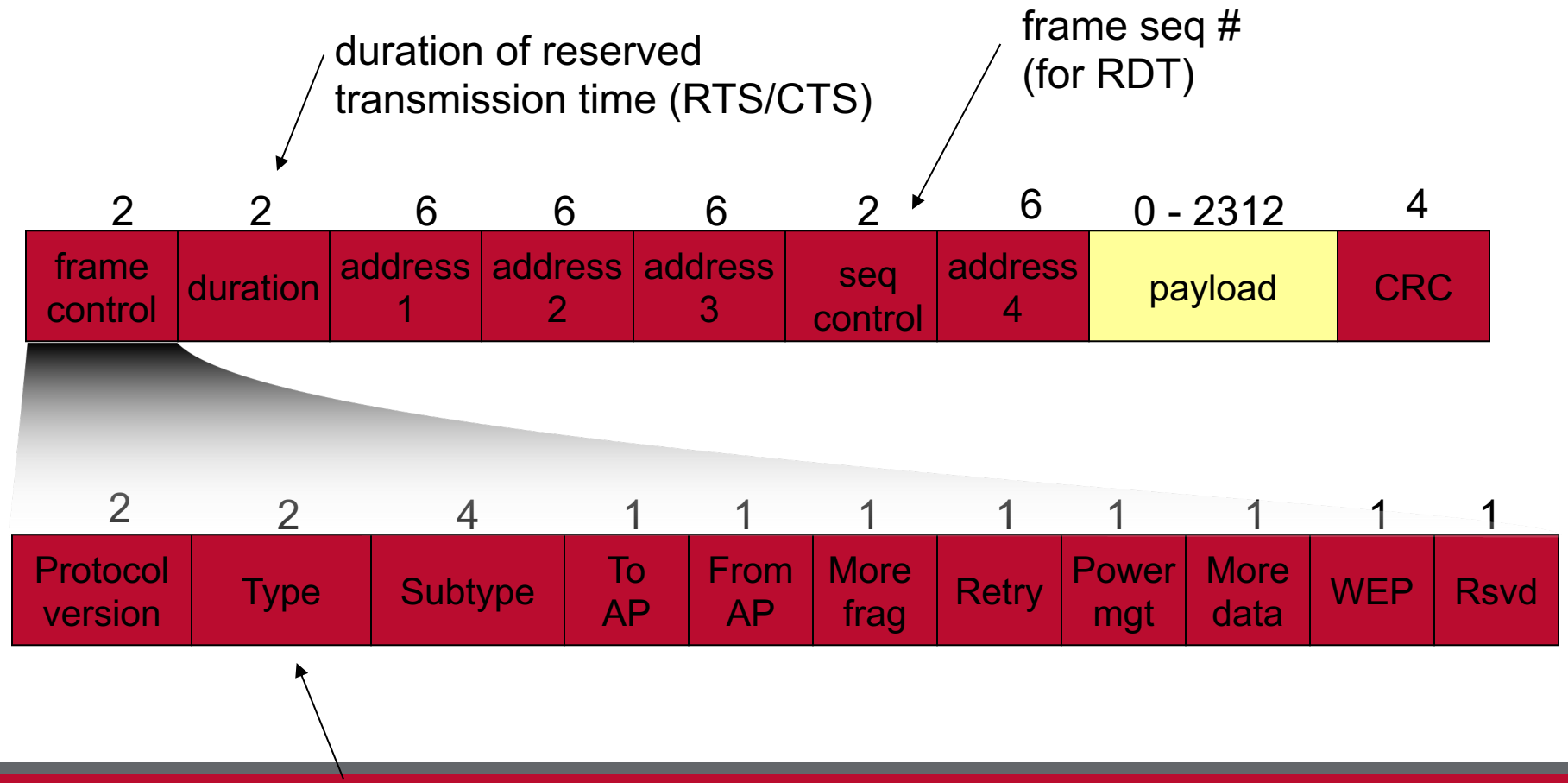
Address 3: MAC address of router interface to which AP is attached

Address 4: used only in ad hoc mode

IEEE 802.11 Addressing



IEEE 802.11 Frame Format (cntd)

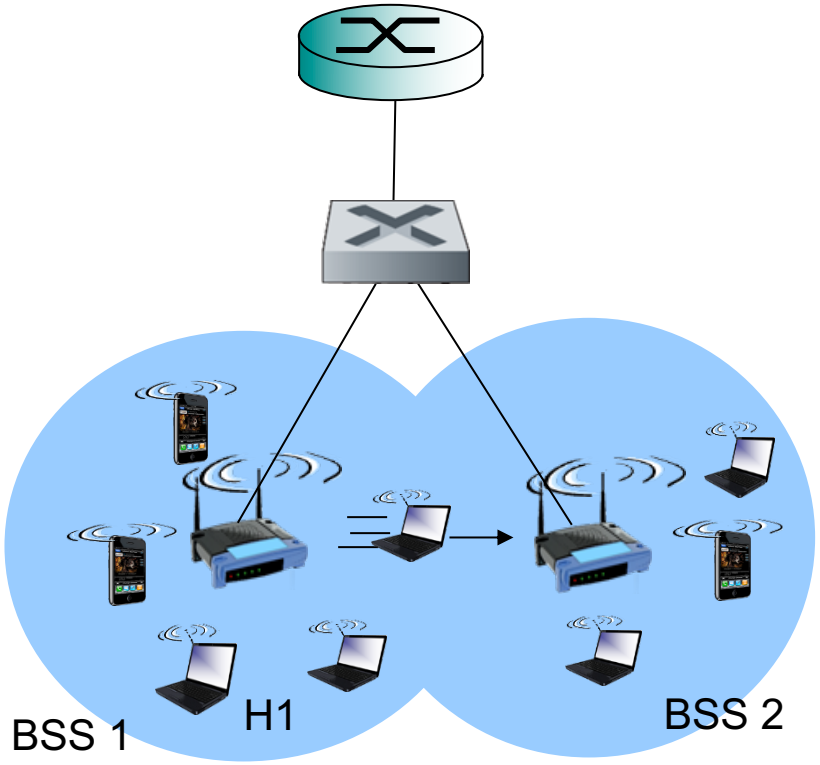


Mobility within the same subnet

H1 remains in same IP subnet: IP address can remain same

switch: which AP is associated with H1?

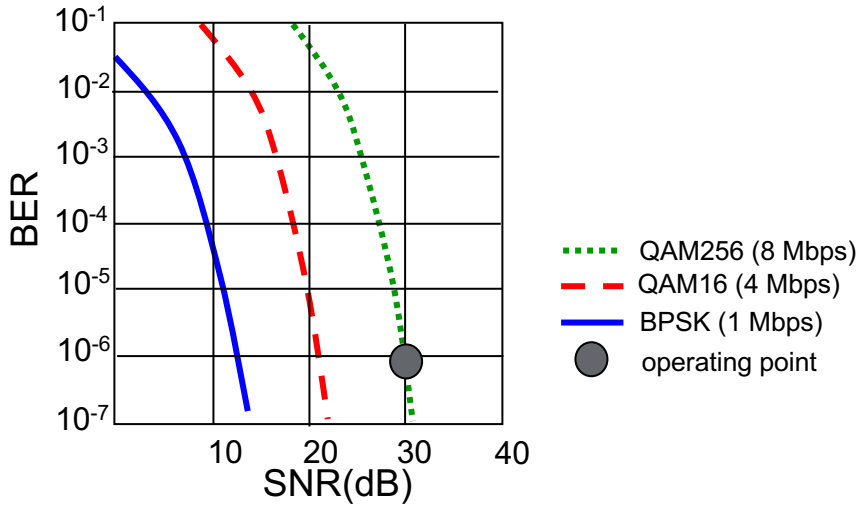
- self-learning: the switch will see frame from H1 and "remember" which switch port can be used to reach H1



IEEE 802.11 Advanced Capabilities

Rate adaptation

- base station, mobile dynamically change transmission rate (physical layer modulation technique) as mobile moves, SNR varies



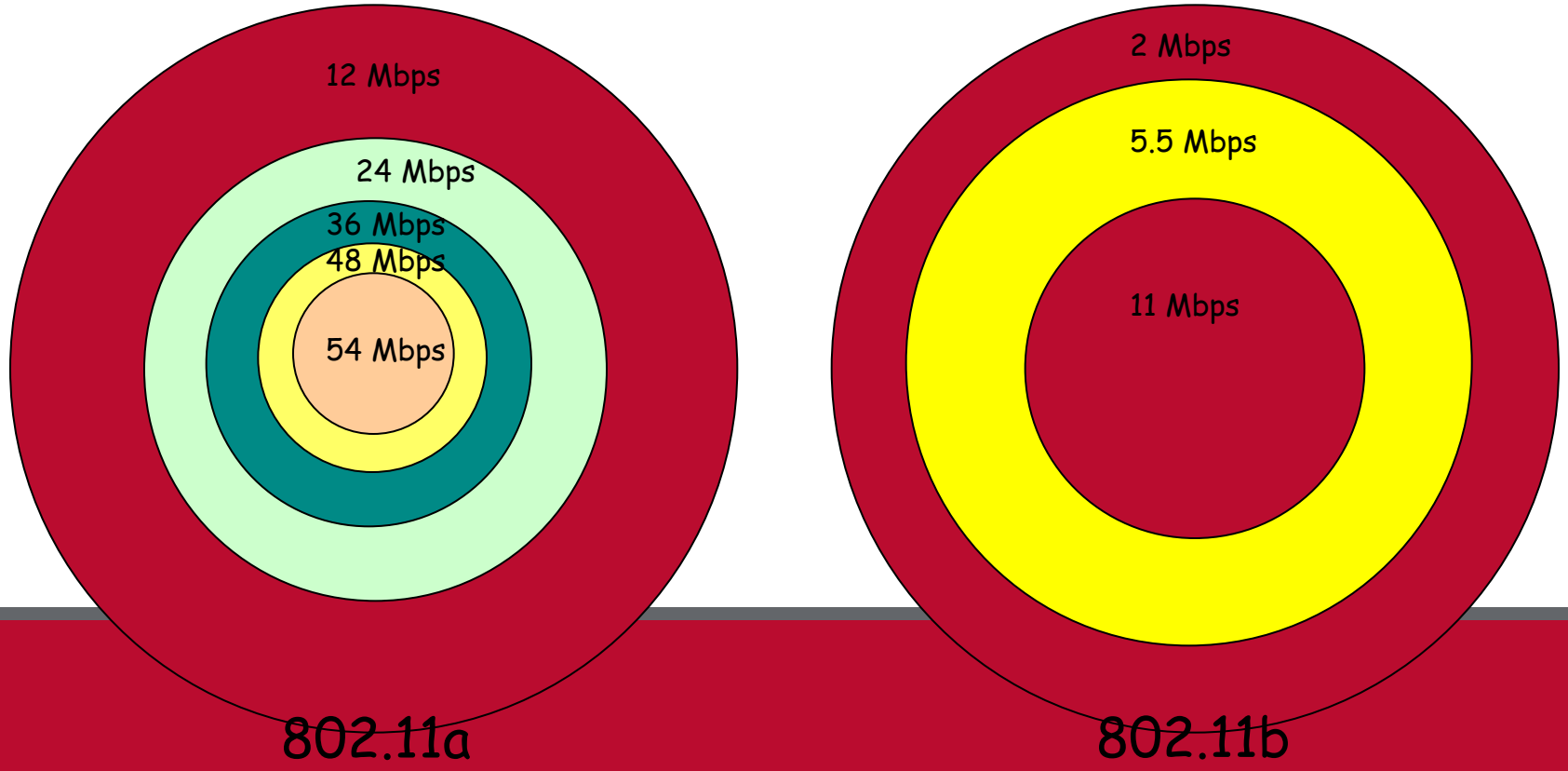
1. SNR decreases, BER increase as node moves away from base station

2. When BER becomes too high, switch to lower transmission rate but with lower BER

IEEE 802.11 Advanced Capabilities

Rate adaptation

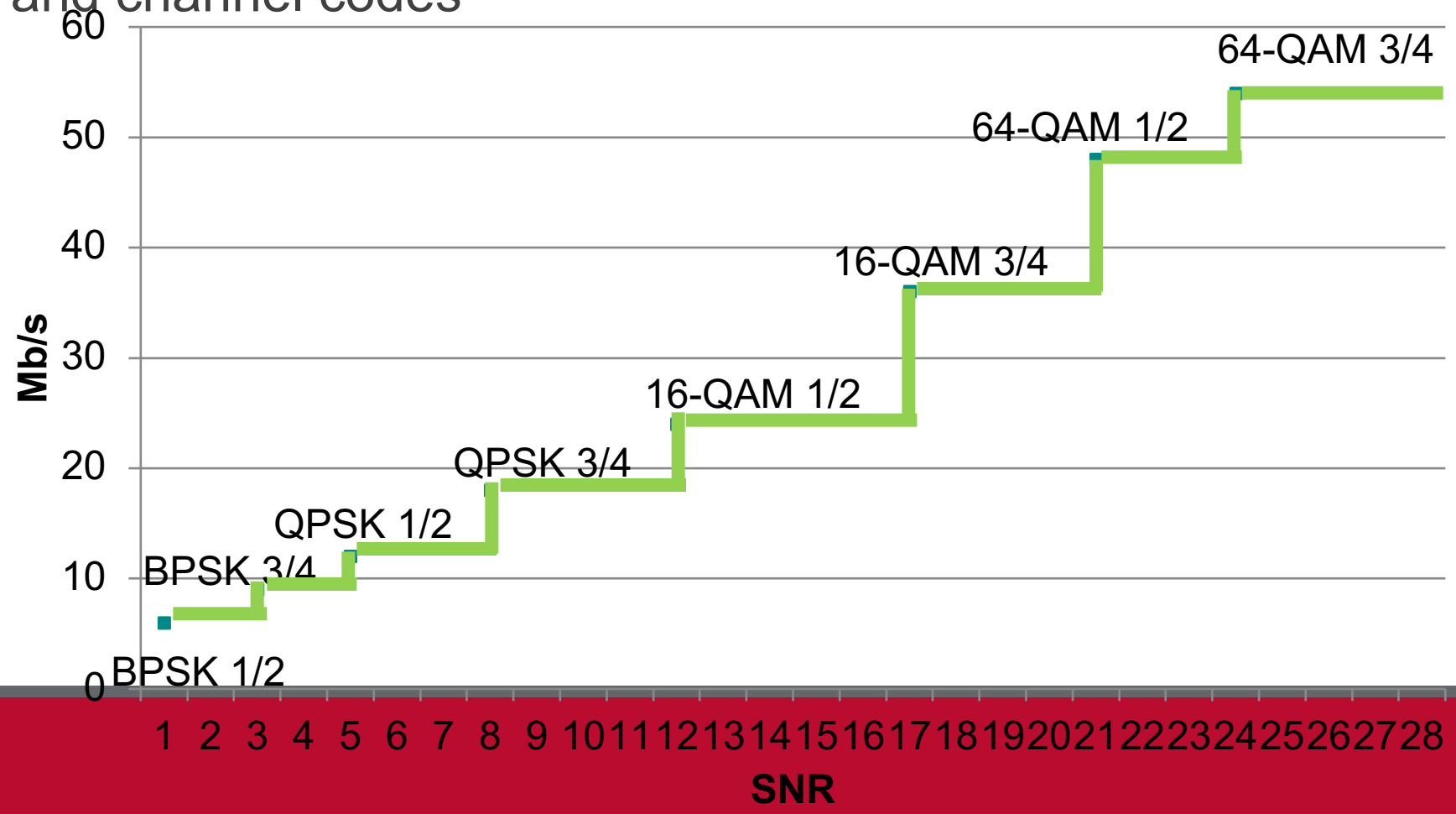
802.11 has a rate fall back mechanism, i.e., as the distance between the transmitter and receiver increases, the supported data rate decreases.



IEEE 802.11 Advanced Capabilities

Rate adaptation

Bitrates and channel codes

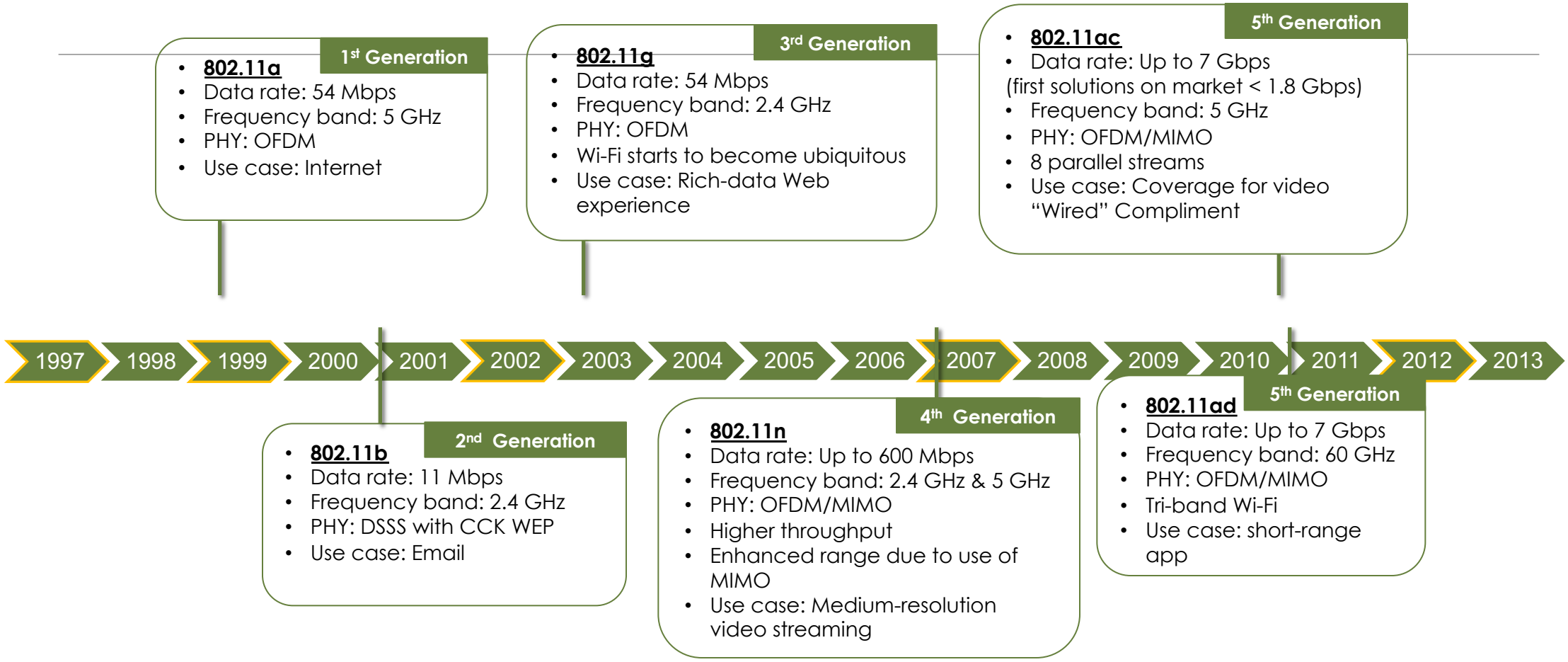


IEEE 802.11 Advanced Capabilities

power management

- node-to-AP: "I am going to sleep until next beacon frame"
  - AP knows not to transmit frames to this node
  - node wakes up before next beacon frame
- beacon frame: contains list of mobiles with AP-to-mobile frames waiting to be sent
  - node will stay awake if AP-to-mobile frames to be sent; otherwise sleep again until next beacon frame

From 1 to 5 – IEEE 802.11 Overview



Modern IEEE 802.11 PHY Protocols

Feature	IEEE 802.11g	IEEE 802.11n	IEEE 802.11ac	IEEE 802.11ad
Channel Bandwidth	20 MHz	20/40 MHz	20/40/80/160 MHz	20/40/80/160/2160 MHz
MIMO Support	No support	Up to 4 streams (4 antennas)	Up to 8 streams (8 antennas)	> 10 streams (> 10 antennas)
Modulation	BPSK/QPSK/16-QAM/64-QAM	BPSK/QPSK/16-QAM/64-QAM	BPSK/QPSK/16-QAM/64-QAM/256-QAM	SQPSK/QPSK/16-QAM/64-QAM
Max PHY Rate	54 Mbps	600 Mbps	7000 Mbps	7000 Mbps
Operating Bands	2.4 GHz	2.4, 5 GHz	5 GHz	2.4, 5, 60 GHz
Beamforming	No support	Supported but not standardized	Standardized	Supported
STBC (space–time block codes)	No support	Many modes and options	Minimized in favour of beamforming	Supported
Range (indoor) (m)	20	70	35	10

Modern IEEE 802.11 MAC protocols